# Privacy and GDPR: Who has my Data

Jose Antigua, CISA, ACDA,COBIT
Director
IT Risk & Assurance

MARCUM
ACCOUNTANTS ▲ ADVISORS
marcumllp.com

# About the speaker: Jose Antigua

## IT Risk & Assurance Director – Southeast region

- More than 11 years of experience in IT Audit, GRC, GRC platform implementation, Security and Data Analytics
- Director for IT Risk & Assurance related services in the Southeast region, including Cybersecurity, IT Governance, Privacy and Compliance
- Certified Information Systems Auditor (CISA), Certified in Governance and Management of IT (COBIT 5) and Data Analysis (ACDA) and trained in "Ethical Hacking and Countermeasures"
- Member of ISACA, the Institute of Internal Auditors (IIA), the International Association of Privacy Professionals (IAPP), Toastmasters International and the FAIR Institute.

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Disclaimer

This publication contains general information only and none of Marcum LLP, any of its related organizations or any of the authors of this publication is, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. Information contained herein is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business.

Evaluation of the information contained herein is the sole responsibility of the user. Before making any decision or taking any action that may affect your business with respect to the matters described herein, you should consult with relevant qualified professional advisors. Marcum LLP, its related organizations and the authors expressly disclaim any liability for any error, omission or inaccuracy contained herein or any loss sustained by any person who relies on this publication.

# Contents

- Context
- Definitions
- Privacy Requirements
- Risks
- Risk Mitigation and Compliance
  - Applicability
  - Data Protection Impact Assessment (DPIA)
  - Implementation
  - Information and Communication
  - Monitoring

MARCUM
ACCOUNTANTS ▲ ADVISORS

# In this digital era…is privacy possible?

- **Tele-density in USA in 2017: 81%**
- **Tele-density in Europe in 2017: 126%**
- **Applications Downloaded worldwide in 2017: 178.1bn**

Our personal data is “out there” being “used” by “someone”.

MARCUM
ACCOUNTANTS ▲ ADVISORS

**Source:**
https://www.statista.com/

# Privacy

**“the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.”**

Generally Accepted Privacy Principles (GAPP), 2009

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Definitions

- Personal Data
- Data Subject
- Data Controller
- Data Processor
- Third Party

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Privacy Requirements

Privacy requirements and frameworks have been around for a while:

- HIPAA (started 1996)
- Asia-Pacific Economic Cooperation (APEC) privacy framework (2005)
- National institute of Standards and Technology (NIST) SP 800-53A Assessing Security and Privacy controls in Federal Information Systems and Enterprises (2008)
- GAPP from the AICPA and CICA (2009)
- OECD (2011)
- ISO 29100 Information Technology – Security Techniques – Privacy framework (2011)
- Privacy Shield (2016)
- General Data Protection Regulation (GDPR) - 2018

# Risks

- **Individuals:** identity theft, black mail, retaliation.

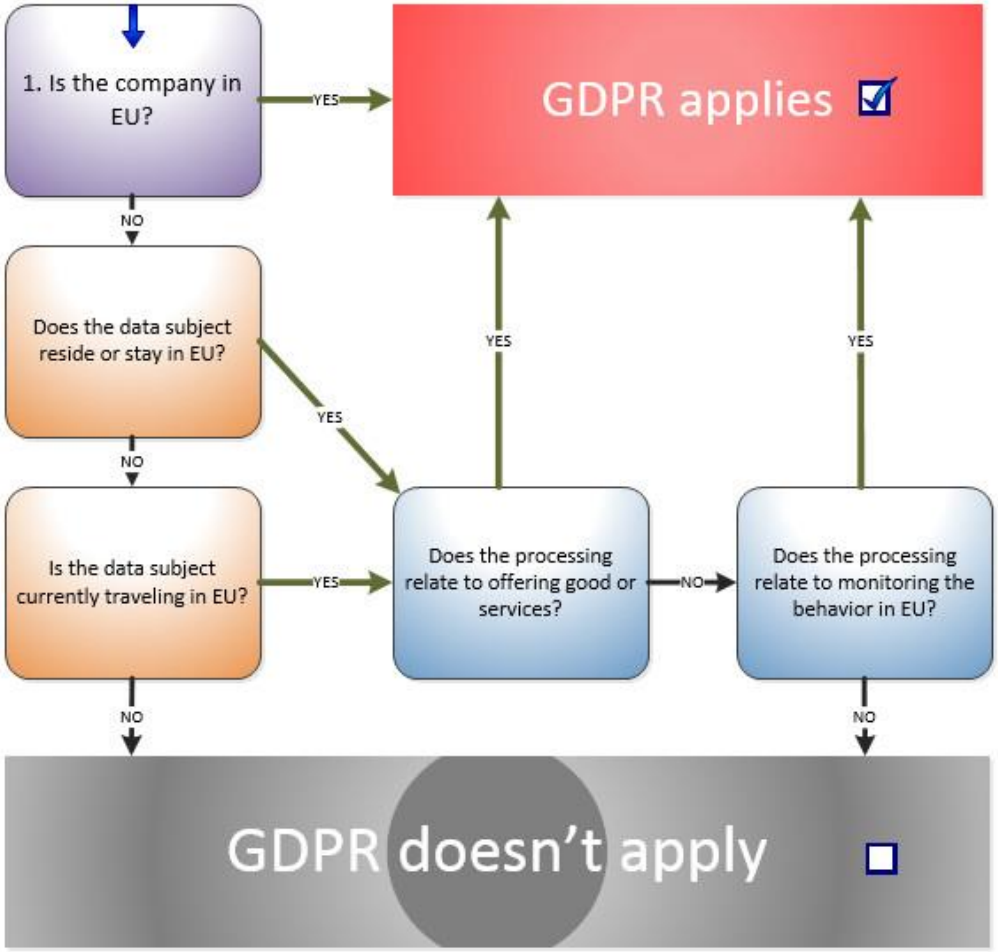
- **Organization:** lawsuit, customer/employee dissatisfaction, interruption of operations, business secret disclosure, fines (up to €20 for GDPR)

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Risk Mitigation and Compliance

- **GDPR:** extraterritorial regulation
- **Overall roadmap to compliance:**
  1. Applicability
  2. Data Protection Impact Assessment (DPIA) – Art. 35
     a) Describe Processing and Scope
     b) Risks to the rights and freedoms of data subjects
     c) Describe mitigating strategies
  3. Implementation
  4. Information and Communication
  5. Monitoring

# 1. GDPR Applicability (Art. 3)




**Source:** Varankevich, Siarhei; "Territorial scope of the GDPR", LinkedIn, 17 February 2017

MARCUM ACCOUNTANTS ▲ ADVISORS

# 2.a - Data Protection Impact Assessment (DPIA) - Describe Process and Scope

Identify **personal data** throughout the organization, in order to determine how much needs to be done. Organize by business area, process, product or other nature. Risk appetite and tolerance will help narrow the task and effort.

Recommended information to document, assuming assessment by process:

- **Process ownership information** *(e.g. process name, owner, dept.)*
- **Related asset(s) with personal data** *(e.g. classification, location)*
- **Assets' type of protection** *(e.g. encryption, behind locked door, etc.)*
- **Types and methods of access to asset** *(e.g. VPN, physical access, email)*

**Once completed, ask:**

"Do we really need this personal data?" and "Do we have explicit business or legal reasons to keep this data?"

*If the answer to any of the questions is "No", start a parallel project to remove and/or stop collecting such data.*

The next step is to understand the risks at each stage of the data lifecycle for every applicable process.

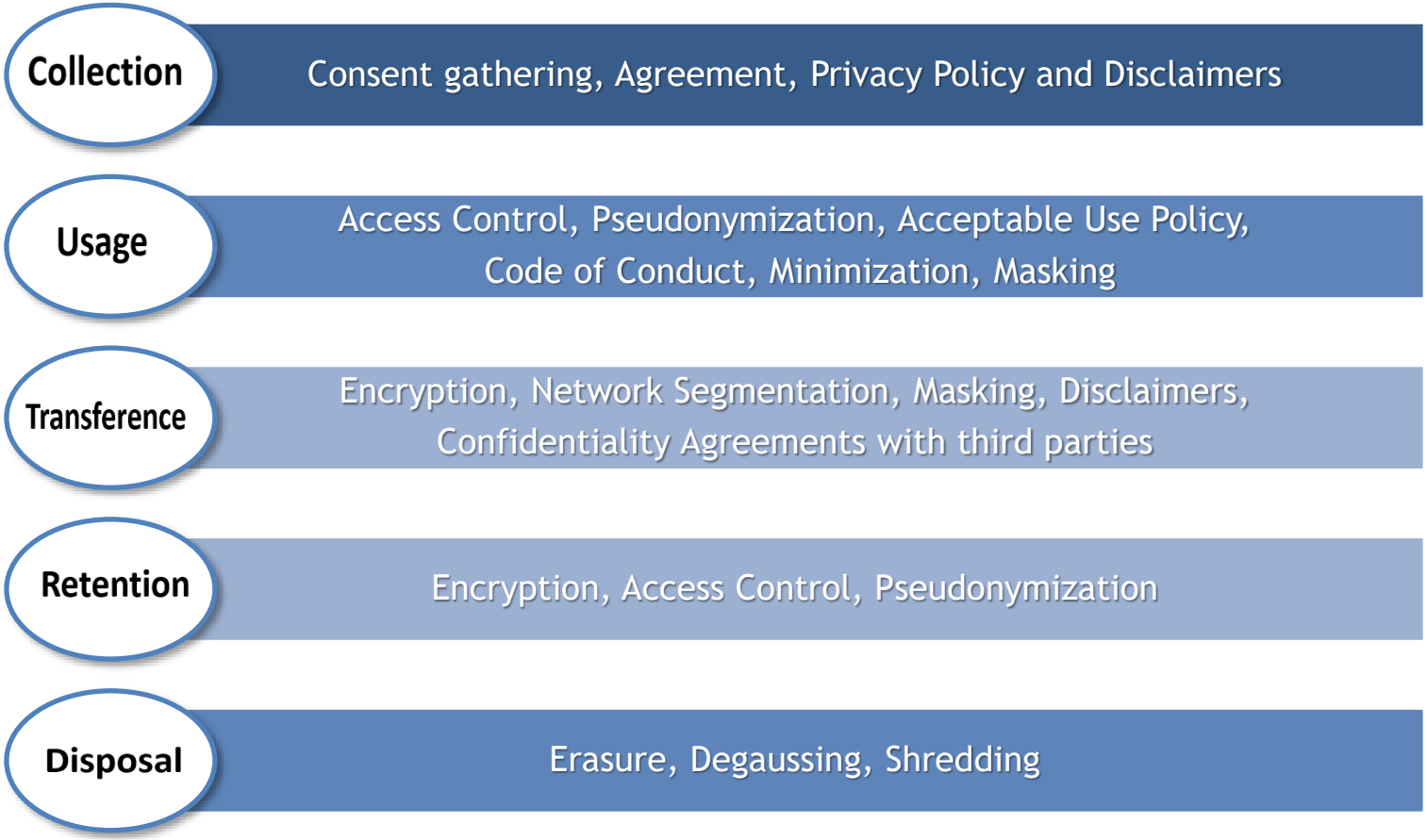
MARCUM
ACCOUNTANTS ▲ ADVISORS

# 2.b - Data Protection Impact Assessment (DPIA) – Examples of Risks to the rights and freedoms of data subjects throughout data lifecycle

| | |
|---|---|
| **Collection** | Unauthorized collection (no explicit, voluntary consent) |
| **Usage** | Unauthorized access, disclosure, unlawful use |
| **Transference** | Data breach, Unauthorized access, unauthorized usage by third parties, violation of right to free movement |
| **Retention** | Unauthorized access, inability to provide “free movement” |
| **Disposal** | Violation of “right to be forgotten”, unauthorized access |

MARCUM
ACCOUNTANTS ▲ ADVISORS

# 2.c - Data Protection Impact Assessment (DPIA) –Examples of Mitigating Strategies throughout data lifecycle




Strategies must also include practices for events where data has been compromised (i.e. breach)

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Implementation considerations

- Integration with existing policies and procedures
- Data Protection by Design (Art. 25)
- Strong third party management program, especially for specific data processors:

*"…the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures…" (Art. 28)*

**Best practices, templates and tools:**

- International Association of Privacy Professionals (IAPP)
- Free guide "Adopting GDPR using COBIT 5" by ISACA

MARCUM
ACCOUNTANTS ▲ ADVISORS

# Information and Communication

- **Metadata about the whole data lifecycle.** From the method and timestamp utilized to obtain consent for data collection, to the log of relevant equipment disposed, every record counts.

- **Awareness and Communication program:**
  - **Internal:** updated code of conduct, acceptable use policies, on-boarding packages and continuous education requirements.
  - **External:** customer and vendor agreements, disclaimers and SLAs.

# Monitoring

- **Self and independent assessments.**

- **Expect possible external assessment by Supervisory Authority (Art. 51).** The supervisory authority has investigative, corrective and advisory powers over the controller or data processor's compliance with the regulation

# Q&A session

MARCUM
ACCOUNTANTS ▲ ADVISORS